CLAIMS

1. A computer system comprising a first node connectable to a second node via one of a plurality of third nodes, communications between the first node and the respective third node being encrypted, and further comprising means for selecting a said third node and setting up an encrypted connection between the first node and the selected third node, means for detecting subsequent failure of the selected third node, and means for selecting another third node and setting up an encrypted connection between the first node and the other selected third node, wherein the first node and the plurality of third nodes form a virtual private network in which communications between the first node and each of the third nodes is encrypted with a respective message encryption key established after an authentication process, wherein the means for selecting the third node comprises a key management service which selects a third node from the plurality and attempts to perform a said authentication process therewith upon a request by the first node for a said message encryption key, and wherein upon successful authentication the said message encryption key is generated and cached at the first node and the selected third node.

2. A computer system as claimed in claim 1, wherein the key management service randomly selects a said third node from the plurality.

3. A computer system as claimed in claim 1, wherein the first node and each of the third nodes includes a respective Internet Protocol (IP) filter which comprises said means for detecting third node failure, wherein the IP filter of the first node sends a failure detection signal to the selected third node, wherein the IP filter of the selected third node sends a response to the failure detection signal if the selected third node is operational, wherein in the event of no said response the IP filter of the first node attempts to find another third node of the plurality which is already authenticated, and will use the respective message encryption key for subsequent communications, or if no other third node is already authenticated, the IP filter of the first node issues a request for a message encryption key to the key management service which attempts to authenticate another third node of the plurality.

4. A computer system as claimed in claim 3, wherein the failure detection signal is transmitted when a respective message encryption key has been established and no communication from the selected third node has been received by the first node within a predetermined time interval.

5. A computer system as claimed in claim 4, wherein when message encryption keys have been established for more than one said third node, the failure detection signal is only sent to the selected third node.

6. A computer system as claimed in claim 4, wherein transmission of the failure detection signal is deferred until after the first node has transmitted encrypted communications to the selected third node.

7. A computer system as claimed in claim 3, wherein the failure detection signal is encapsulated in the same manner as the communications between the first node and the selected third node are configured, and the response of the selected third node comprises an equal signal in the opposite direction.

8. A computer system as claimed in claim 2, wherein the key management service randomizes the order of the plurality of third nodes as listed in a policy file of the first node, and an IP filter of the first node searches the randomized list in sequential order when attempting to find another third node for communications therewith.

9. A method of detecting node failure, and connecting to another node, in a computer system comprising a first node connected to a second node via one of a plurality of third nodes, communications between the first node and the one said third node being encrypted, the method being employed for detecting failure of the one said third node, after authentication and connection of the first node thereto, and for establishing connection of the first node to another of said third nodes, and including steps wherein the first node sends a failure detection signal to the one said third node at a predetermined time, wherein if the one said third node is operational it sends a response to the failure detection signal to the first node,

wherein in the event of the receipt of no said response within a predetermined time interval the first node either establishes a connection with another said third node which was previously authenticated, or attempts to authenticate another said third node and establish connection therewith, and wherein the first node and the plurality of third nodes form a virtual private network in which communications between the first node and each of the third nodes is encrypted with a respective message encryption key, and the method includes the step of establishing a respective message encryption key after each said authentication.

10. A method as claimed in claim 9, and including the steps of randomly selecting a third node from the plurality upon a request for a message key by the first node, performing an authentication process with the selected third node, and if successful generating a said message encryption key and caching it at the first node and the selected third node.

11. A method as claimed in claim 10, wherein the failure detection signal is transmitted when a respective message encryption key has been generated and no communication from the selected third node has been received by the first node within the predetermined time interval.

12. A method as claimed in claim 10, wherein when message encryption keys have been established for more than one said third node, the failure detection signal is only sent to the selected third node.

13. A method as claimed in claim 10, wherein transmission of the failure detection signal is deferred until after the first node has transmitted encrypted communications to the selected third node.